DTEX
WORKFORCE CYBER INTELLIGENCE

SOLUTION BRIEF

Insider Threat & Data Loss Protection for Servers

IDENTIFY MALICIOUS ACTIVITY

PROTECT SERVERS FROM COMPROMISE

PREVENT DATA EXFILTRATION

DTEX InTERCEPT provides comprehensive server security with complete visibility, predictive analytics and prevention capabilities.

In today's distributed, cloud-centric enterprise, it's harder than ever before to find and stop insider and external emerging threats. Organizations continue to protect their critical server infrastructure and sensitive IP with point security solutions that lack the comprehensive protection and visibility needed in today's threat landscape.

Comprehensive Server Protection with DTEX InTERCEPT

DTEX InTERCEPT is a Workforce Cyber Security solution that replaces legacy User Activity Monitoring, Internal Forensics, DLP and User Behavior Analytics tools with a lightweight, cloud-native platform that has near-zero impact on server performance. Powered by DTEX's patent-pending DMAP+ Technology™, **InTERCEPT** continuously collects hundreds of unique elements of enterprise telemetry from data, machines, applications and people.

Only DTEX InTERCEPT protects cloud, on-premise and virtual servers from data breaches, insider threats and outsider infiltration with unparalleled visibility, detection and scalability. InTERCEPT provides real-time visibility into all server activity as it relates to a user, and applies advanced analytics to discern legitimate activity from malicious "Indicators of Intent," including those commonly associated with data loss such as reconnaissance, obfuscation and circumvention activities. This delivers accurate awareness and the ability to pinpoint threats early in the kill chain to identify risks before exfiltration attempts.

KEY USE CASES

- Critical File Integrity Monitoring
- Data Loss Protection
- Identification of Unusual Account Behavior
- Unexpected Server Access
- Privileged Account Monitoring
- Bastion/Jump Host Monitoring
- Rogue & Shadow IT Application Detection

See alerts for malicious, compromised or suspicious behaviors occurring on server environments.

Quickly understand high-risk service and user accounts.

Easily spot when and what suspicious activities are occurring across your servers.

SOLUTION BRIEF

Insider Threat & Data Loss Protection for Servers

DTEX InTERCEPT – Continuous Server Monitoring at Scale

See and stop SolarWinds Orion and other legitimate software-based attacks

As reported by cybersecurity firm FireEye in December 2020, hackers inserted "malicious code into legitimate software updates for the SolarWinds Orion software that allowed an attacker remote access into a victim's environment" with reported "indications of compromise dating back to the spring of 2020." The attack reportedly leveraged a backdoor in a SolarWinds library, maintained on an organization's server infrastructure, which was initiated when an update to SolarWinds was applied.

Traditional cyber defense methods fall short and do not provide visibility of these kill chain behaviors prior to a breach and customer exposure. DTEX InTERCEPT can and does. For example, with DTEX InTERCEPT, cybersecurity and IT teams get real-time visibility to understand the behavior types that occur on servers as a result of SolarWinds Orion-type attacks.

- **Minimal malware:** the presence of malware TTPs that make the attack vector difficult to detect via traditional means
- **Stealth:** attempts to avoid detection by blending into normal network activity (e.g., trusted certificates, etc.)
- **Reliance on administrative tools:** use of administrative tools to conduct reconnaissance and cover tracks makes profiling of anomalous behavior of superuser accounts on endpoints and servers paramount

> ***We evaluated five solutions against a weighted criteria of 13 must-have capabilities, including user behavior monitoring within specialty engineering applications and a collector that was invisible to employees. DTEX InTERCEPT was the only solution that gave us those lightweight collection capabilities and the visibility we need to support our mission-critical operational requirements."***
>
> ***Graeme Hackland***
> *Chief Information Officer, WIlliams Racing*

WILLIAMS RACING

FEATURE HIGHLIGHTS

SERVER SECURITY
Privileged Account Misuse
File Integrity Monitoring (FIM) Contextualization
SWIFT Server Monitoring
Unusual Application Behavior
Unusual Database Behavior
Unusual Privilege Escalation
Bastion/Jump Server Monitoring
Unusual Service Account Behavior

MALICIOUS BEHAVIOR
Bypass of Security Controls
Unusual Privilege Escalation
Obfuscation & Covering Tracks
Unauthorized Use of Administrative/Cyber/Hacking Tools
Flight Risk & Data Loss
On/Off-Network Monitoring
Portable Application Use

COMPROMISED BEHAVIOR
(MITRE ATT&CK)
Unusual Privilege Escalation
JSP Backdoor Detection
Domain Fronting
Lateral Movement
ToR & Proxy Bypass
Malicious or Unusual Application Behavior
Unusual Data Aggregation

NEGLIGENT BEHAVIOR
Teachable Moment Reporting
Accidental Data Loss
Use of Non-Sanctioned Software
Online File-Sharing Misuse
Shadow IT
Bulk Transfer Utilities
Instant-Messaging Usage

RISK, AUDIT & COMPLIANCE
Automated Risk Reporting (Benchmark & Baseline)
Inappropriate Internet Usage
Use of Personal Webmail
System Configuration Changes
Unauthorized Use of Decommissioned Accounts and/or Assets
Business Continuity Reporting
Use of Non-Sanctioned Software
Unauthorized Use of Communication Software

DATA LOSS PROTECTION
Wireless Transfers (e.g., Airdrop/Bluetooth)
USB Device Usage
Instant-Messaging Applications
Upload to Cloud Storage (Online File-Sharing)
Personal vs. Corporate Webmail (e.g., G Suite)
Printing
FTP/sFTP/SCP
Confidential/Sensitive File Transfers

FORENSIC INVESTIGATIONS
Audit Trail of All Activities
Leavers Forensic Audit (365)
Joiners Forensic Audit (Probation Period)
File Lineage
Rogue Applications
Abnormal Internet Activity
DMAP Contextual Audits (Data, Machines, Applications, People)
User to Admin Account Correlation

SUPPORTED PLATFORMS

Microsoft · Linux · macOS® · CITRIX®

REQUEST A DEMO

Contact us today to schedule a demonstration
demo@dtexsystems.com

About DTEX Systems

DTEX Systems is the world leader in Workforce Cyber Intelligence and committed to helping enterprises run safer and smarter. Only DTEX dynamically correlates data, application, machine, and human telemetry to stream context-rich user behavior and asset utilization analytics that deliver a first-of-its-kind human-centric approach to enterprise operational intelligence. Hundreds of the world's largest enterprises, governments and forward-thinking organizations leverage DTEX to prevent insider threats, stop data loss, maximize software investments and deployments, optimize workforce productivity, and protect remote workers. DTEX has offices in San Jose, California and Adelaide, South Australia and is backed by Northgate Capital, Norwest Venture Partners, Wing Ventures, and Four Rivers Group. To learn more visit: www.dtexsystems.com.